SAW/MSM:cmw 3382-53699-01 142331.01 855536 05/21/08

KLARQUIST SPARKMAN, LLP
16th Floor World Trade Center, 121 S.W. Salmon Street, Portland, Oregon 97204 U.S.A.
PHONE: 503-595-5300 FAX: 503-595-5301

PLEASE DELIVER DIRECTLY TO EXAMINER YIN CHEN SHAW

Fax No.: 571-270-8593

Total No. Pages: 7 including this cover sheet

Message: Transmitted herewith for filing in the below-identified application is an Interview Agenda. If you do not receive all pages or if you have problems receiving transmittal, please call Stephen A. Wight at (503) 595-5300.

In re application of: Goland
Application No. 09/882,491
Filed: June 15, 2001
Confirmation No. 8148
For: NETWORKED DEVICE BRANDING FOR SECURE INTERACTION IN TRUST WEBS ON OPEN NETWORKS
Examiner: Yin Chen Shaw
Art Unit: 2135
Attorney Reference No. 3382-53699-01

FAXED ON:
MAY 21, 2008

INTERVIEW AGENDA

As per the telephone conference between the Examiner and Ryan Fox on May 21, 2008, Applicants have agreed to a telephonic interview at 2:00 PM EDT on May 26, 2008. Applicants will telephone the Examiner at that time. In preparation for the interview, Applicants provide this agenda with draft claim amendments provided solely for the purpose of discussion.

In the Office action dated December 31, 2007, the Examiner allowed independent claim 2 (below) over Hind and Doneti. Although the Examiner did not elaborate over which language he found distinguishing over the prior art, (*see*, Office action, page 9), Applicant has added emphasis on the features that were amended in the Office action response immediately prior to allowance:

> 2. A branding process to establish cryptographically secured interaction among networked computing devices within a trust group, the trust group comprising a group of devices, on an open multi-access network,

comprising:

securely networking a security-uninitialized device with a branding device via a secured network medium;

generating a branding certificate *at* the branding device, the branding certificate instructing that the security-uninitialized device trust the branding device, the branding certificate further containing key data for verifying certificates provided by other devices on the open multi-access network to the security-uninitialized device are authenticated by the branding device;

transmitting the branding certificate from the branding device to the security-uninitialized device via the secured network medium;

generating a trust group membership certificate *at the branding device* which is signed by the branding device, the trust group membership certificate containing a signed group name as well as a signed key identifying the security-uninitialized device such that, when the security-uninitialized device sends the trust group certificate to a branded device which is a member of the trust group, the trust group certificate is validated by the branded device, and the branded device verifies that the security-uninitialized device identified in the trust group membership certificate is a member of the trust group of devices referred to by the group name;

transmitting the trust group membership certificate from the branding device to the security-uninitialized device via the secured network medium; and

initializing a security resolver of the security-uninitialized device to use the key data of the branding certificate to authenticate other devices interacting with the security-uninitialized device on the open multi-access network are in the trust group, and to provide the trust group membership certificate to such other devices as authentication that the security-uninitialized device is a member of the trust group, such that at least some interaction via the open multi-access network with the security-uninitialized device is cryptographically secured to only other devices in the trust group.

Independent claim 13 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Hind in view of Dondeti. Applicant suggests the following amendments to independent claim 13 which incorporates language similar to that from independent claim 2:

13. A networked computing device supporting branding to establish cryptographically secured interaction with other devices within a trust group of devices on an open-access network, the networked computing device comprising:

a network interface for communicating on the open-access network;

a security resolver operational after being initialized with a branding public key to authenticate trust group membership certificates separate from the branding public key provided to the networked computing device from other devices via the network interface using the branding public key, and further operational to inhibit interaction via the network interface with other devices not authenticated as in the trust group of devices, the security resolver being initially

uninitialized; and

a security initializer operational to receive the branding public key from a branding device securely networked to the networked computing device, the branding device having previously generated the branding public key and trust group membership certificates, and the branding device having transmitted the branding public key and the trust group membership certificates to the security initializer over a secured network medium, and the security intializer being further operational to initialize the security resolver with the branding public key.

Applicant believes that amended independent claim 13 as proposed is allowable over the cited prior art and looks forward to discussing the proposed language with the Examiner. Please call the undersigned if any further information is required.

Stephen A. Wight
Registration No. 37,759

May 21, 2008
Date